

REMARKS

Claims 1-5 were examined. All claims were rejected. In response to the above-identified Office Action, Applicants amend the application and seek reconsideration thereof.

I. Claims Rejected Under 35 U.S.C. § 112, Second Paragraph

The Examiner rejected Claims 1-5 under 35 U.S.C. § 112, second paragraph, for failing to point out and distinctly claim the subject matter which applicants regard as the invention. Each Claim was rejected for a specified linguistic error. In this Response, Applicants amend each Claim to improve clarity of expression and conform to standard English usage. Applicants respectfully request that this ground of rejection be withdrawn.

II. Claims Rejected Under 35 U.S.C. § 102(b)

The Examiner rejected Claims 1 and 4 under 35 U.S.C. § 102(b) as anticipated by *Schneier* in Applied Cryptography (“*Schneier*”). In order to anticipate a claim, the reference must teach each limitation of the claim. In view of the present amendments, Applicants respectfully submit that *Schneier* fails to anticipate Claims 1 and 4 for the following reasons.

As to Claim 1, the Examiner attempts to establish a concordance between the parties and steps discussed at page 54 of *Schneier* and the elements of Claim 1, in order to show that *Schneier* anticipates the claim. However, because the reference and the claim describe their respective protocols from different viewpoints, the concordance must be constructed very carefully. As the following discussion will show, the protocols are actually different in purpose and execution. Thus, *Schneier* fails to disclose each and every element of Claim 1, and therefore does not anticipate it.

Claim 1 refers to a method for defeating a denial-of-service attack for use in a communication system, in which a client and a server perform certain calculations and send or receive certain messages. *Schneier* discloses a secure proof-of-identity protocol by means of which “Alice” can verify her identity to a host. The Examiner’s analysis considers “Alice” to be the client of Claim 1, and the host to be the server of Claim 1. Comparing the protocols with this assignment of roles in mind, one may align *Schneier*’s

step (1), “Alice performs a computation ... and sends the result to the host” with Claim 1 (a), “[the server receives] a service request from a client.” In response, in *Schneier*’s step (2), “the host sends Alice a different random number,” while Claim 1 (a) requires the server to generate a random number r_B and send it to the client.

At this point, however, the methods diverge. In *Schneier* step (3), “Alice makes some computation based on the random numbers ... and her private key, and sends the result to the host.” In Claim 1 (b), the server receives a ciphertext produced by the client using the random number r_B from the server and a random number r_A selected by the client, enciphered with the public key of the server. Two entirely different ciphertexts are created in *Schneier* step (3) and Claim 1 (b). The Examiner will appreciate that the use of a party’s own private key creates a different message, with different security and authentication properties, than does the use of another party’s public key. At a minimum, Alice can decrypt the message she sends to the host, while the client in Claim 1 cannot; furthermore, Alice’s message proves to the host that she possesses the private key corresponding to her public key, while the client’s message from the protocol in Claim 1 proves only that the client can receive a random number, generate a random number, and encrypt the two using the server’s public key.

The methods continue to diverge in subsequent steps. In *Schneier* step (4), “[t]he host does some computation on the various numbers received from Alice and her public key to verify that she knows her private key.” However, in Claim 1 (c), the server recovers a random number from the ciphertext received from the client based on the private key of the server and compares the recovered random number with the random number sent to the client. The server in Claim 1 (c) does not, and indeed *cannot*, verify that the client knows its own private key based on the message it receives from the client, because it has received nothing encrypted with the client’s private key.

For at least these reasons, Applicants respectfully submit that the method of *Schneier* is different than the method of Claim 1. Therefore, the rejection of Claim 1 as anticipated by *Schneier* should be withdrawn.

As to Claim 4, Claim 4 recites a computer readable medium for recording a program for implementing functions that, for the purpose of the current analysis, are similar to the method of Claim 1. In particular, a client sends a service request to a server, which responds by generating a random number r_B and sending it to the client. The client produces a ciphertext based on the random number r_B and a random number r_A , and sends the ciphertext to the server. The server recovers a random number from the ciphertext and compares it to the random number the server sent earlier, and provides service if the recovered and sent random numbers are equal, or denies service if they are unequal.

These steps vary from those taught by *Schneier* for the same reasons as those discussed with respect to Claim 1: the messages are prepared differently and prove different propositions. Although there is a superficial similarity between the methods, the similarity extends no further than the number of parties and the fact that some sort of encrypted communication occurs between them. The details of the communications are quite different, and it is clear that *Schneier* fails to teach every limitation of Claim 4.

For at least the foregoing reasons, Applicants believe that Claims 1 and 4 are not anticipated by *Schneier*, and respectfully request that these rejections be withdrawn.

III. Claims Rejected under 35 U.S.C. § 103(a)

The Examiner rejected Claims 2, 3 and 5 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,910,989 issued to Naccache (“*Naccache*”) in view of *Schneier* (*supra*). Applicants respectfully disagree.

As to Claim 2, Applicants note initially that Claim 2 depends upon Claim 1. As discussed above, Claim 1 is patentable over *Schneier*, so Claim 2 (which incorporates all of the limitations of Claim 1) is likewise patentable. In addition, although *Naccache* is somewhat cryptic, it appears that the portion cited by the Examiner uses a hash function to generate a signature complement, using as inputs a secret key x , a random element J that is generated at the outset by the card and stored in the card to be used when the “coupon” is to be used to establish a signature, and an index i representing the number of

the coupon used. The hash function in *Naccache* uses a random element (J), but does not appear to *produce* a random number, as Claim 2 requires.

As to Claims 3 and 5, Applicants object to the official notice of using exponentials as a common way to encrypt or decrypt a ciphertext. If such use of exponentials becomes relevant to the examination of Claims 3 or 5, the Examiner is requested to locate an appropriate reference. However, in regard to the current rejections of Claims 3 and 5 under 35 U.S.C. § 103(a) as obvious over *Schneier* in view of *Naccache*, Applicants suggest that it is irrelevant whether the use of exponentials for encryption is well-known. In order to establish a *prima facie* case of unpatentability, the Examiner must show that there is some suggestion or motivation in the references or general knowledge to combine or modify the references, that there is a reasonable expectation of success from such combination or modification, and that the references teach or suggest all the claim limitations. MPEP § 2143. Applicants respectfully submit that this has not been done in the rejections of Claims 3 and 5.

As to Claim 3, Claim 3 recites a method for defeating a denial-of-service attack comprising several specified steps. The Examiner has not identified specific discussion in any cited reference that teaches or suggests those steps. Thus, no *prima facie* case has been made.

As to Claim 5, Claim 5 recites a computer readable medium for recording a program for implementing several specified functions. The Examiner has not identified specific discussion in any cited reference that teaches or suggests those functions. Thus, no *prima facie* case has been made.

Furthermore, in the present invention, the client encrypts a random number r_B received from the server as well as its own random number r_A based on the server's public key in order to check whether the client generates a ciphertext under a protocol. In other words, for defeating denial-of-service attacks on authentication protocols, the client is verified by generating and sending the ciphertext based on the random numbers r_A and r_B and the server's public key. However, *Schneier* and *Naccache* fail to teach encrypting

the random number r_A of the client and the random number r_B of the server based on the server's public key.

For at least the foregoing reasons, Applicants believe that Claims 2, 3 and 5 are patentable over *Naccache* in view of *Schneier*. Therefore, the Examiner is respectfully requested to withdraw these rejections.

The Examiner also rejected Claims 1-5 under 35 U.S.C. § 103(a) as unpatentable over Juels *et al.* In "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks" ("*Juels*"). Applicants respectfully disagree that the claims are obvious in view of *Juels*.

While it is true that *Juels* describes a method of blocking a denial of service attack by sending a puzzle from the server to the client, where the client must return the correct solution in order to gain access to the system, *Juels* does not describe the methods for defeating denial-of-service attacks claimed in Applicants' invention. In fact, *Juels* notes that "[f]inding more efficient puzzle constructions represents an interesting research problem" (§ 3.4), and the Examiner has done no more to construct a *prima facie* case of unpatentability than take official notice that inverse functions and hashing are well known in the art and assert that "it would have been obvious to one of ordinary skill in the art that the inverse functions on a hashed key would be possible puzzles in Jules' method."

Applicants respectfully request that the Examiner provide references in support of the proposition that inverse functions and hashing are well known, and a reference that teaches or suggests using inverse functions and hashing in the manner claimed herein.

In the absence of such references, Applicants submit that the rejection of Claims 1-5 under 35 U.S.C. § 103(a) as obvious over *Jules* is improper, and request that this ground of objection be withdrawn.

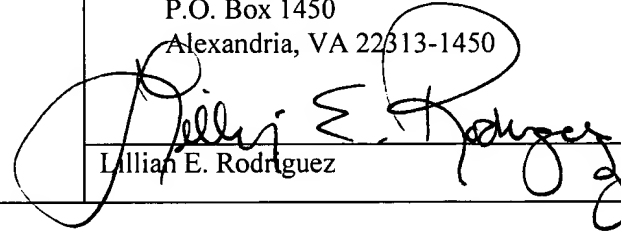
CONCLUSION

In view of the foregoing, it is believed that all claims now pending, namely Claims 1-5, patentably define the subject invention over the prior art of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207-3800.

Dated: 9/24, 2004

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP


Eric S. Hyman, Reg. No. 30,139

<p>12400 Wilshire Boulevard Seventh Floor Los Angeles, California 90025 (310) 207-3800</p>	<p style="text-align: center;"><u>CERTIFICATE OF MAILING</u></p> <p>I hereby certify that the correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:</p> <p style="text-align: center;">Mail Stop Amendment Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450</p> <p> 9-24-04 Lillian E. Rodriguez September 24, 2004</p>
---	---